---

de Freitas, Sara and Levene, Mark (2005). Spam. *In* Claude Ghaoui ed. *Encyclopedia of Human Computer Interaction*. Hershey, Pa.; London: Idea Group Reference (an imprint of Idea Group Inc.), pp. 553-558.

Encyclopedia of Human Computer Interaction

Claude Ghaoui
Liverpool John Moores University, UK

Idea Group REFERENCE

IDEA GROUP REFERENCE
Hershey · London · Melbourne · Singapore

Acquisitions Editor: Michelle Potter
Development Editor: Kristin Roth
Senior Managing Editor: Amanda Appicello
Managing Editor: Jennifer Neidig
Copy Editors: Shanelle Ramelb and Sue VanderHook
Typesetters: Diane Huskinson
Support Staff: Sharon Berger, Amanda Kirlin, and Sara Reed
Cover Design: Lisa Tosheff
Printed at: Yurchak Printing Inc.

Published in the United States of America by
Idea Group Reference (an imprint of Idea Group Inc.)
701 E. Chocolate Avenue, Suite 200
Hershey PA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@idea-group.com
Web site: http://www.idea-group-ref.com

and in the United Kingdom by
Idea Group Reference (an imprint of Idea Group Inc.)
3 Henrietta Street
Covent Garden
London WC2E 8LU
Tel: 44 20 7240 0856
Fax: 44 20 7379 0609
Web site: http://www.eurospanonline.com

Library of Congress Cataloging-in-Publication Data

Encyclopedia of human computer interaction / Claude Ghaoui, Editor.
p. cm.
Summary: "This encyclopedia presents numerous experiences and insights, of professional from around the world, on human computer interaction issues and perspectives"--Provided by publisher.
Includes bibliographical references and index.
ISBN 1-59140-562-9 (hardcover) -- ISBN 1-59140-798-2 (ebook)
1. Human-computer interaction--Encyclopedias. I. Ghaoui, Claude.
QA76.9.H85E 52 2006
004'.019--dc22

2005031640

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

Spam

Sara de Freitas
Birbeck College, University of London, UK

Mark Levene
Birbeck College, University of London, UK

INTRODUCTION

With the advent of the electronic mail system in the 1970s, a new opportunity for direct marketing using unsolicited electronic mail became apparent. In 1978, Gary Thuerk compiled a list of those on the Arpanet and then sent out a huge mailing publicising Digital Equipment Corporation (DEC—now Compaq) systems. The reaction from the Defense Communications Agency (DCA), who ran Arpanet, was very negative, and it was this negative reaction that ensured that it was a long time before unsolicited e-mail was used again (Templeton, 2003). As long as the U.S. government controlled a major part of the backbone, most forms of commercial activity were forbidden (Hayes, 2003). However, in 1993, the Internet Network Information Center was privatized, and with no central government controls, spam, as it is now called, came into wider use.

The term *spam* was taken from the Monty Python Flying Circus (a UK comedy group) and their comedy skit that featured the ironic spam song sung in praise of spam (luncheon meat)—"spam, spam, spam, lovely spam"—and it came to mean mail that was unsolicited. Conversely, the term *ham* came to mean e-mail that was wanted. Brad Templeton, a UseNet pioneer and chair of the Electronic Frontier Foundation, has traced the first usage of the term *spam* back to MUDs (Multi User Dungeons), or real-time multi-person shared environment, and the MUD community. These groups introduced the term *spam* to the early chat rooms (Internet Relay Chats).

The first major UseNet (the world's largest online conferencing system) spam sent in January 1994 and was a religious posting: "Global alert for all: Jesus is coming soon." The term *spam* was more broadly popularised in April 1994, when two lawyers, Canter and Siegel from Arizona, posted a message that advertized their information and legal services for immigrants applying for the U.S. Green Card scheme. The message was posted to every newsgroup on UseNet, and after this incident, the term *spam* became synonymous with junk or unsolicited e-mail. Spam spread quickly among the UseNet groups who were easy targets for spammers simply because the e-mail addresses of members were widely available (Templeton, 2003).

BACKGROUND

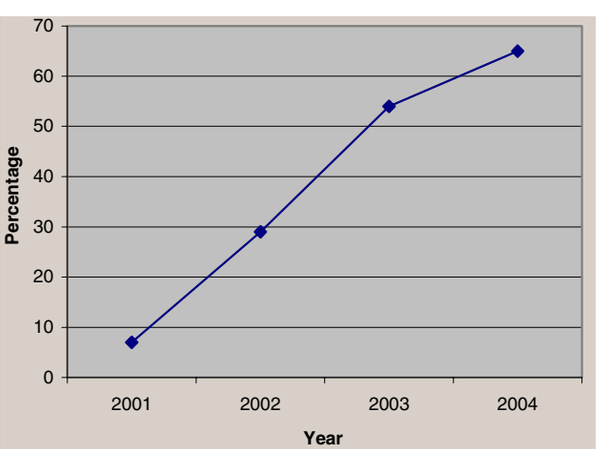
At present, the practice of spamming is pervasive; however, due to the relative recent nature of the problem and due to its fast changing nature, the discussion about the topic has been limited to academic literature. While in computer science literature there has been a concentration of work on the technical features and solutions designed to prevent or ameliorate the practice (Androutsopoulos et al., 2000; Gburzynski & Maitan, 2004; Goodman & Rounthwaite, 2004), the more general scientific discussion has been provided by a few scientific commentators (Gleick, 2003; Hayes, 2003), and the few books written on the subject (Schwartz & Garfinkel, 1998) have become outdated in a relatively short span of time. In other academic areas, there is some literature available concerning the legal implications of spam (Crichard, 2003) and the marketing dimension of spamming (Nettleton, 2003; Sipior et al., 2004); however, these, too, have suffered from the fast changing and global scope of the problem. Furthermore, aspects such as the social and political implications of spamming have been restricted to journalistic commentary in newspaper articles (BBC News, 2003, 2004; Gleick, 2003; Krim, 2004). In order to provide a broader focus in this article, therefore, the authors have supplemented this literature with interviews conducted with spe-

cialists in the field in order to provide the most up-to-date information, including interviews with Enrique Salem, CEO of Brightmail; Mikko Hyponnen of F-Secure; and Steve Linford of the Spamhaus Project.

However, while the broader issues of spamming have been discussed in the general literature reviewed, in the area of human-computer interaction, there has been a paucity of discussion, although this may change with the wider take-up of mobile devices with their context awareness. Notable articles that have touched on related issues in the human-computer interaction field have included those that have considered issues of privacy (Ackerman et al., 2001) and usability in particular difficulties with using computer technology (Kiesler et al., 2000). However, this is not to say that spamming does not play a role in reversing the convenience that many experience when using e-mail on their desktop, laptop, or mobile device, and it is often the most vulnerable that are affected adversely by spamming practice.

The mass appeal and use of electronic mail over the Internet has brought with it the practice of spamming or sending unsolicited bulk e-mail advertising services. This has become an established aspect of direct marketing, whereby marketers can reach many millions of people around the world with the touch of a button. However, this form of direct marketing or spamming, as it has come to be called, has become an increasing problem for many, wasting people's time as they delete unwanted e-mail and slowing down the movement of electronic traffic over local and wide area networks (Salem interview, 2004; Goodman & Rounthwaite, 2004).

Graph 1. The escalation of spam worldwide, 2001 to July 2004 (Source: Brightmail)



The scale of the problem has become particularly concerning in recent months; unsolicited e-mail—or spam—currently accounts for 65% of all e-mail received in July 2004 (Brightmail, 2004; Enrique Salem, CEO of Brightmail, interview 2004). Of the 70 million e-mails that Brightmail filtered in September 2003 alone, 54% was unsolicited, and that percentage is increasing year after year (see Graph 1). But although there are a number of different ways to filter unwanted e-mail, which may lead to a significant reduction of spam in the short term, many experts in the field are concerned that spam will never be completely eradicated (Hypönnen, F-Secure interview, 2004; Linford, Spamhaus interview, 2004).

CRITICAL ISSUES OF SPAM

So who are the spammers? The spammers can be identified in three main groups: (1) legitimate commercial direct marketers, who want to make commercial gain from sending bulk e-mails about products and services; (2) criminal groups, including fraudsters, who are using spam to "legitimise"' their activities and to defraud others (Gleick, 2003; Levy, 2004; Linford interview, 2004); and (3) disaffected individuals—crackers—who want to disrupt Internet services and who, in many cases, may have inside information about how the systems are structured. The criminal group is potentially the most dangerous, and while spam is not an illegal activity, this practice is set to spread to the criminal fraternity in China, Russia, and South America. This trend is becoming more widespread with the ease of obtaining spam kits over the Internet, which allows the potential spammer to set up quickly (Thomson, 2003).

Increasingly, illegitimate spammers, fraudsters, and crackers are joining forces to introduce fraud schemes such as the 419 scam and phishing (sending e-mails as if they came from trusted organisations) to convince unsuspecting victims to reveal sensitive personal information; in particular, to gain information about users' credit card information or to gain access details of online transaction services (Levy, 2004).

WAYS OF COMBATING SPAM

In the light of this increasing problem, a series of attempts, both technological and non-technological, have been made to try to combat the annoyance of full mailboxes in order to counter the heavyweight of unwanted e-mail traffic and to deter criminal activity (Goodman & Rounthwaite, 2004). Hand in hand with the push for tighter legislation to tackle the problem, several technical solutions have been deployed, and new ones are being proposed.

Before an e-mail arrives in your mailbox it passes through a mail server, which is either hosted within your organization or through an Internet Service Provider (ISP). Filtering out spam at this early stage (pre-receipt) before the message arrives at your machine is obviously desirable, and many IT departments and ISPs already have installed anti-spam software on their servers. Tools also exist that are user-based and filter out e-mail that already has arrived at your mailbox (post-receipt). Due to the flood of spam that is relentlessly sent to us, for now, it is probably best to have filtering tools both at the server and the user ends.

Two problems that need to be addressed by any spam filtering system are the rates of false positives and false negatives. A false positive is a mail message that the filter tags as spam but is actually ham, while a false negative is a mail message that the filter tags as ham but is actually spam. Having no filter at all is the case of 0% false positives and 100% false negatives, and a filter that blocks everything is one with 100% false positives and 0% false negatives. Ideally, we want 0% false positive (i.e., all ham gets through the filter) and 0% false negatives (i.e. all spam is blocked).

The methods for combating spam include the following, which are summarized in tabular form (see Table 1).

- Blocklisting
- Protocol change
- Economic solutions
- Computational solutions
- E-mail aliasing
- Sender warranted e-mail
- Collaborative filtering
- Rule-based solutions
- Statistical solutions
- Legislative solutions

All these methods for combating spam impede the usability of e-mail and necessitate extra technical and administrative support; however, the safety and security for individuals using Internet and e-mail-based services is reliant upon controlling the misuse of the systems; therefore, these methods are a trade-off between free and open access and secure and safe systems. Of course, there are social and political implications for employing these preventative methods; however, there is clearly a need to address these failings using more than one listed method.

There is clearly a need to consider the problem of spam in the human-computer interaction field, particularly relating to issues of increasing usability for more vulnerable user groups, such as those with particular disabilities, frailties, and illnesses, who may be particularly susceptible to particular scams and fraudulent deceits.

FUTURE TRENDS

Future areas of development for spamming may center upon relatively unprotected mobile phones and devices (Sipior et al., 2004; Syntegra, 2003). To date, the practice known as *wardriving*, where individuals drive around until they detect wireless connectivity and then bombard the unprotected network with spam, provides a real indication about the potential dangers of spamming for the future. Another concerning trend has been the use of spam to send out viruses (Stewart, 2003), the SoBig virus attack, for example, that used this method.

In addition, the cheap and easy availability of spam kits that provide mailing lists and the spamming software on the Internet have spread the practice to new territories, in particular to China, Russia, and South America, making the practice more widespread and leading to an escalation in the rate of spamming.

Other adaptations of the spamming practice recently have included the use of malicious code, using worms and trojans spam relays are created; the MyDoom worm operated in this way, installing proxies that spammers could then exploit.

Table 1. Methods for combating spam

Solution	Method	Benefits	Limitations
Block listing	Use of lists of IP addresses of known sources of spam (e.g., SBL and RBL)	Blocks a significant volume of spam	Cannot block all spam and needs to be updated on a regular basis
Protocol change	To provide a method of tracking the source of an e-mail	Will help to identify spammers and add spam addresses to block lists	Will not prevent spam as such
Economic solutions	Impose a fee for sending e-mail	Will deter spammers from sending large volumes of junk e-mail	Will be difficult and costly to implement a worldwide standard for collecting the fee
Computational solutions	Impose an indirect payment in the form of a machine computation prior to sending e-mail	It is a viable alternative to the economic solution, without needing the infrastructure to collect a fee	A protocol involving cryptographic techniques will need to be put in place and software developed to implement the method
E-mail aliasing	Set up e-mail aliases for different groups of people with different acceptance criteria	Will reduce spam through an authentication process	This method involves an extension to current e-mail servers and the management of e-mail aliases
Sender warranted e-mail	Use of a special header to certify the e-mail as valid	No need for additional software or e-mail protocol	Will probably not deter spammers if widely adopted, and wide licensing of the technology will be problematic
Collaborative filtering	Communities collaborate to fight spam using a collaborative tool that is an add-on to e-mail software	Possible eradication of large volumes of spam through collaborative reporting of spam	Still vulnerable to random changes in spam e-mail, and there are problems with scalability of this method
Rule-based solutions	These filters maintain a collection of patterns to be matched against incoming spam, as in SpamAssassin	It is easy to install and effective in blocking a large percentage of spam, and in the case of SpamAssassin, it is free	It needs a lot of tuning and should be combined with other methods to filter out a larger volume of spam
Statistical solutions	Often deployed as a post-receipt spam filter using Bayesian text classification to tag e-mail as spam or ham	It is very effective and also adaptive, so it is hard to fool	Most effective when used with other pre-receipt filter systems
Legislative solutions	National and global legislation to enforce anti-spam laws	Prosecution of individual spammers	Problems of enforcement, not least due to crossing of different jurisdictional boundaries

The increase in the technical sophistication of spammers also is evidenced by the use of so-called reputation attacks, where spammers use a worm to launch a denial of service attack against anti-spamming organisations. One such example was the Mimail attacks (Levy, 2004) that specifically targeted anti-spam organisations seeking to block out spam. Clearly, spamming is becoming more refined and will evolve to adapt to any perceived weaknesses in network security.

CONCLUSION

This article has highlighted the scale and depth of the spamming problem, and while many are committed to the eradication of all Internet-based fraud and illegitimate activity, it seems unlikely that spam will completely disappear. It is more likely that the practice will continue to evolve and transmute to adapt to new vulnerabilities in the systems and to exploit users who are not fully aware of how they can be exploited through impersonations of familiar Web sites and services. With the current force behind the anti-spam movement gaining momentum, we can expect to see less spam in the future, but only with preventative measures such as those described in this article being put in place. In the near future however, the cat-and-mouse game among spammers and anti-spammers is set to continue. In particular, the new routes for spammers clearly lie in reaching users through mobile devices, which need to become

better protected by virus and spam software, if these cyber crimes are to be controlled and ameliorated.

REFERENCES

Ackerman, M., Darrell, T., & Weitzner, D.J. (2001). Privacy in context. *Human-Computer Interaction, 16*, 167-176.

Androutsopoulos, I., Koutsias, J., Chandrinos, K.V., & Spyopoulos, C.D. (2000). An experimental comparison of naïve Bayesian and keyword-based anti-spam filtering with personal e-meal messages. *Proceedings of the 23rd Annual International ACM SIGIR Conference on Research and Development in Information Retrieval*, Athens, Greece.

BBC News. (2003). *Top UK sites fail privacy test*. Retrieved August 1, 2004, from http://news.bbc.co.uk/2/hi/technology/3307705.stm

BBC News. (2004). *US anti-spam law fails to bite*. Retrieved August 1, 2004, from http://news.bbc.co.uk/2/low/technology/3465307.stm

Brightmail. (2004). Retrieved August 1, 2004, from http://www.brightmail.com/spamstats.html

Crichard, M. (2003). Privacy and electronic communications. *Computer Law and Security Report, 19*(4), 299-303.

Gburzynski, P., & Maitan, J. (2004). Fighting the spam wars: A re-mailer approach with restrictive aliasing. *ACM Transactions on Internet Technology, 4*(1), 1-30.

Gleick, J. (2003). Get out of my box. *Guardian Review,* 1-2.

Goodman, J., & Rounthwaite, R. (2004). Stopping outgoing spam. *Proceedings of the 5th ACM Conference on Electronic Commerce*, New York.

Hayes, B. (2003). Spam, spam, spam, lovely spam. *American Scientist, 91*(3), 200-204.

Hypönnen, M. (personal communication, February 27, 2004)

Kiesler, S., Zdaniuk, B., Lundmark, V., & Kraut, R. (2000). Troubles with the Internet: The dynamics of help at home. *Human-Computer Interaction, 15*, 323-351.

Krim, J. (2004, May 21). Senate hears mixed reviews of anti-spam law. *Washington Post*. Retrieved August 1, 2004, from http://www.washingtonpost.com/wp-dyn/articles/A43622-2004May20.html

Levy, E. (2004). Criminals become tech savvy. *IEEE Security and Privacy, 2*(2), 65-68.

Linford, S. (personal communication, January 9, 2004)

Nettleton, E. (2003). Electronic marketing and the new anti-spam regulations. *The Journal of Database Marketing and Customer Strategy Management, 11*(3), 235-240.

Salem, E. (personal communication, February 23, 2004)

Schwartz, A., & Garfinkel, S. (1998). *Stopping spam.* Beijing: O'Reilly and Associates.

Sipior, J.C., Ward, B.T., & Bonner, P.G. (2004). Should spam be on the menu? *Communications of the ACM, 47*(6), 59-63.

Stewart, J. (2003). Spam and SoBig: Arm in arm. *Network Security,* 12-16.

Syntegra. (2003). *Can spam kill the mobile messaging market?* [white paper]. Retrieved August 1, 2004, from http://www.us.syntegra.com/acrobat208950.pdf

Templeton, B. (2003). Brad Templeton Home Page. Retrieved October 29, 2003, from www.templetons.com/brad/spam react.html

Thomson, I. (2003). *Mafia muscles in on spam and viruses*. Vnunet.com. Retrieved Aptil 26, 2004, from http://www.vnunet.com/News/1151421

KEY TERMS

Blocklisting: Set up as an approach for blocking unsolicited or junk e-mail. Blocklists provide lists of URLs or Web addresses from which spammers operate. The blocklists therefore provide a way of ameliorating or preventing spam from reaching the intended destination.

E-Mail Aliasing: Where an individual has more than one e-mail address, the practice allows the user to use different addresses for different tasks; for example, one address for Internet communications and another for business.

False Negatives: A false negative is a mail message that the filter tags as ham but is actually spam.

False Positives: A false positive is a mail message that the filter tags as spam but is actually ham.

Phishing: Short for password harvest fishing, it is the process of impersonating another trusted person or organization in order to obtain sensitive personal information, such as credit card details, passwords, or access information.

Sender Warranted E-Mail: This method allows the sender to use a special header to certify that the e-mail is genuine. The process could help to prevent spam scams.

Spam: Otherwise termed unsolicited e-mail, unsolicited commercial e-mail, junk mail, or unwanted mail, it has been used in opposition to the term *ham*, which is wanted e-mail. The term was developed from a Monty Python comedy sketch depicting spam as useless and ham as lovely, albeit in ironic terms.

Wardriving: Also termed WiLDing—Wireless Lan Driving, it is an activity whereby individuals drive around an area detecting Wi-Fi wireless networks, which they then can access with a laptop.